18.30

Abgeordneter David Stögmüller (Grüne): Sehr geehrte Frau Präsidentin! Sehr geehrte Frau Rechnungshofpräsidentin! Werte Kolleginnen und Kollegen! Make the world a better place. – Wissen Sie, von wem das ein Slogan ist? Aktuell sehen Sie, wenn Sie derstandard.at aufmachen, ganz oben einen Header mit Vulkan-Files.

Vulkan-Files ist ein Netzwerk von Hackern, ein GRU-Netzwerk, da reden wir von russischen Geheimdiensten, dem GRU, dem FSB, dem SWR. Das sind Geheimdienste mit dem Hackerkollektiv Sandworm.

Warum ist das so interessant? Warum ist das so gefährlich? – Heute war Präsident Selenskyj hier und hat vor einem massiven Hackerangriff auf Europa und auf die Welt gewarnt. Genau dieses Netzwerk wurde heute entlarvt. Das geschah vor ein paar Stunden durch ein Kollektiv von deutschen und österreichischen Medien – ARD, „Der Spiegel“, „Der Standard“ – und einem quasi neuen Netzwerk, einem Investigativnetzwerk, nämlich paper trail media. Die haben entlarvt, wie brutal Russland im Hackerbereich vorgeht: Desinformation, Fakeprofile, Zensur, Maßnahmen zur Überwachung nach Innen sowie nach Außen, gezieltes Aufspüren von Schwachstellen in den Infrastrukturen anderer Länder. Es wurden Schweizer AKWs, Außenministerien und ukrainische Botschaften genannt, die als Schwachstellen identifiziert wurden. Nun wurde auch – und das ist das Besondere – der Angriff auf das österreichische Außenministerium genannt.

Genau das ist der Punkt, der mich heute zum Rechnungshofbericht reden lässt: Diese Schwachstelle, die durch den Angriff auf das österreichische Außenministerium entdeckt wurde, findet sich nämlich exakt im Rechnungshofbericht wieder. Diese Schwachstelle ist ein massives Problem. Seit 2013 gibt es dieses Cyberprofil und eine österreichische Sicherheitsstrategie, die nie adaptiert worden ist. Das ist auch ein Punkt, der dringend notwendig ist, weil da Cyber nur peripher genannt wird. Auch die Cyber-Sicherheitsstrategie von 2013

war schon damals, 2019, als der Cyberangriff auf das österreichische Außenministerium war, komplett überholt. Es ist dringend notwendig, dass da etwas passiert.

Das Frühwarnsystem, das vom Netz- und Informationssicherheitsgesetz vorgesehen war, war 2021 von der Umsetzung auch noch weit entfernt. Auch da müssen wir angasen, da müssen wir etwas umsetzen. Dass die Koordination der verschiedenen Organe mangelhaft war und weder die Länder noch das Digitalisierungsministerium irgendwie in die operative Koordination eingebunden waren, war einer der Kritikpunkte des Rechnungshofes.

Ich zitiere noch einen Punkt aus Ihrem Bericht, Frau Präsidentin: Räumlichkeiten und sonstige Ausstattungen wie Hardware und Software waren nicht vorhanden und müssten um 2 Millionen Euro notbeschafft werden. – So, und nun kommt ja der Clou in dieser ganzen Geschichte, und das finde ich ja das besonders Spannende. Wir haben heute Selenskyj gehört, wir wissen nun Bescheid über russische Netzwerke, über die Hackerangriffe. Wir wissen, mit welcher Brutalität Russland im Netz agiert.

Was machte dazumals das Außenministerium? Es gibt ein Netzwerk in Deutschland, also es gibt verschiedenste, aber der Deutsche Nicolaus von Rintelen mit Virtual Solution, einem Netzwerk rund um Jan Marsalek – wir wissen ja, Marsalek hat engste Verbindungen nach Russland, das ist alles relativ gut bewiesen –, versucht, in das Außenministerium zu lobbyieren, nämlich den Auftrag zu bekommen, dass sie diese Cyberattacke von 2019 bewältigen. Nein, man kam noch drauf. Man hat dann diesen Auftrag einer anderen Firma gegeben, nämlich Cyan Networks; wieder ein Auftrag von über 1,69 Millionen Euro. Cyan Networks wurde bei Ihnen Firma B genannt. Diese Firma gehört lustigerweise wieder zum Netzwerk von Jan Marsalek und dem Netzwerk von Russland.

Genau das ist unser Problem: Wir beschäftigen immer wieder russische Netzwerke und russische Firmen, ohne das irgendwie zu checken. Bei uns gibt es Intransparenz in genau diesen Problemlagen. Es gibt kein Problembewusstsein, welche Firmen wofür engagiert werden. Das muss notwendigerweise passieren.

Da ist nur Dsurf zu nennen, eine österreichische Firma mit engsten Netzwerken nach Russland und Aufträgen in die Geheimdienste. Das steht alles in langen Zeitungsartikeln, es stand vor drei Wochen im „Profil“, große Artikel. Wir haben da kein Problembewusstsein. Wenn dieser Angriffskrieg von Russland eines bedeutet, dann: Wir müssen in Österreich Problembewusstsein bekommen! *(Beifall bei Grünen und NEOS.)*

Ja, es werden fast täglich neue Technologien entwickelt, und die bringen nicht nur Gefahren, sondern auch Chancen. Nützen wir die Chancen, erkennen wir die Gefahren und agieren wir auch dementsprechend! – Frau Präsident, ich bin Ihnen sehr dankbar für diesen Bericht, denn Sie zeigen schonungslos auf, dass wir in diesem und auch in vielen anderen Bereichen wirklich noch Nachholbedarf haben. Bitte bleiben Sie da auch in Ihrer Cyberabteilung dran, denn gerade diese Netzwerke nach Russland und in Drittländer, die eine Gefahr für die österreichische Sicherheitsstruktur darstellen, müssen restlos aufgeklärt werden – nicht nur in finanzieller Hinsicht, sondern auch darüber hinaus, nämlich ob es eine Struktur ist, der wir vertrauen können. – Vielen Dank dafür. *(Beifall bei Grünen und NEOS.)*

18.36

Präsidentin Doris Bures: Nächster Redner: Herr Abgeordneter Hoyos-Trauttmansdorff. – Bitte.